



(12)实用新型专利

(10)授权公告号 CN 208521346 U

(45)授权公告日 2019.02.19

(21)申请号 201821115742.9

(22)申请日 2018.07.13

(73)专利权人 湖南创合未来科技股份有限公司

地址 410001 湖南省长沙市雨花区环保中路169号

(72)发明人 曹明威 伍军辉

(74)专利代理机构 北京集佳知识产权代理有限公司 11227

代理人 罗满

(51)Int.Cl.

G07C 9/00(2006.01)

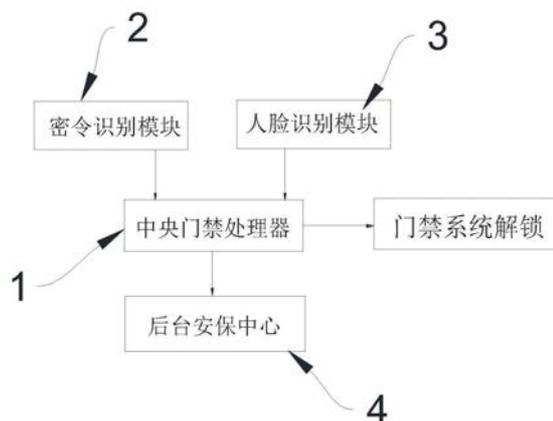
权利要求书1页 说明书5页 附图2页

(54)实用新型名称

一种具备反胁迫功能的人脸识别门禁系统

(57)摘要

本申请公开一种具备反胁迫功能的人脸识别门禁系统,包括:中央门禁处理器;密令识别模块,用于识别接收的密令为常态正确密令或反胁迫密令,若为反胁迫密令则发送异常胁迫信号至中央门禁处理器;人脸识别模块,用于验证人脸信息特征通过后发送解锁指令至中央门禁处理器;中央门禁处理器用于接收人脸识别模块发送的解锁指令,控制门禁系统解锁;以及,用于接收密令识别模块发送的反胁迫指令,将反胁迫信息发送至后台安保中心。本申请提供的一种具备反胁迫功能的人脸识别门禁系统,与现有技术相比,极大程度上保障了工作人员的人身安全以及国家财产安全,安全性得到了显著提高。



1. 一种具备反胁迫功能的人脸识别门禁系统,其特征在于,包括:
中央门禁处理器;
密令识别模块,用于识别接收的密令为常态正确密令或反胁迫密令,若为反胁迫密令则发送异常胁迫信号至所述中央门禁处理器;
人脸识别模块,用于验证人脸信息特征通过后发送解锁指令至所述中央门禁处理器;
所述中央门禁处理器用于接收所述人脸识别模块发送的解锁指令,控制门禁系统解锁;以及,用于接收所述密令识别模块发送的反胁迫指令,将反胁迫信息发送至后台安保中心。
2. 根据权利要求1所述的具备反胁迫功能的人脸识别门禁系统,其特征在于,所述人脸识别模块包括:摄像单元,用于采集人脸图像;识别单元,用于从所述摄像单元采集的图像中检测识别出人脸图像;提取单元,用于从采集的图像中提取人脸图像;预处理单元,用于对提取出来的人脸图像进行预处理;计算模块,用于计算待识别人员与已录入人员特征的卡方值;匹配识别单元,用于验证待识别人员的身份,验证用户信息通过后发送发送解锁指令至所述中央门禁处理器。
3. 根据权利要求2所述的具备反胁迫功能的人脸识别门禁系统,其特征在于,所述人脸识别模块还包括:归一化处理单元,用于对预处理后的人脸图像进行归一化处理;特征提取单元,用于从归一化的人脸图像中提取待识别人员的特征。
4. 根据权利要求3所述的具备反胁迫功能的人脸识别门禁系统,其特征在于,所述中央门禁处理器用于接收所述密令识别模块发送的反胁迫指令,将反胁迫信息发送至安保后台管理中心具体为:中央门禁处理器将由所述摄像单元采集的现场实时照片以及视频传送至后台安保中心。
5. 根据权利要求3所述的具备反胁迫功能的人脸识别门禁系统,其特征在于,所述人脸识别模块还包括位姿调整提示单元,用于在所述人脸识别模块验证人脸特征信息失败后,发送提示验证人员调整位姿,再次进行人脸采集的提示信息。
6. 根据权利要求1所述的具备反胁迫功能的人脸识别门禁系统,其特征在于,所述密令识别模块具体为指纹密令识别模块。
7. 根据权利要求6所述的具备反胁迫功能的人脸识别门禁系统,其特征在于,所述指纹密令识别模块包括:指纹录入单元,用于录入用户常态开锁指纹信息以及异常胁迫指纹信息;指纹识别及信息处理单元,用于识别实时输入的指纹信息为常态开锁指纹信息或异常胁迫指纹信息,若识别为异常胁迫指纹信息则向所述中央门禁处理器发送异常胁迫信号。
8. 根据权利要求1所述的具备反胁迫功能的人脸识别门禁系统,其特征在于,所述密令识别模块具体为数字密码识别模块。
9. 根据权利要求8所述的具备反胁迫功能的人脸识别门禁系统,其特征在于,数字信息输入部,用于输入数字信息,数字密码识别及信息处理模块,用于识别实时输入的数字信息为常态开锁密码信息或异常胁迫密码信息,若识别为异常胁迫密码信息则向所述中央门禁处理器发送异常胁迫信号。
10. 根据权利要求1所述的具备反胁迫功能的人脸识别门禁系统,其特征在于,具备反胁迫功能的人脸识别门禁系统还包括验证记录保存模块,所述验证记录保存模块用于保存验证人员的现场验证人脸照片,以及验证时间信息。

一种具备反胁迫功能的人脸识别门禁系统

技术领域

[0001] 本申请涉及人脸识别技术领域,更具体地说,尤其涉及一种具备反胁迫功能的人脸识别门禁系统。

背景技术

[0002] 人脸识别技术为一种利用分析比较人脸视觉特征信息,以进行身份鉴别的计算机技术。随着计算机技术与图像处理技术的飞跃发展,人脸识别技术应运而生,并在公共安全领域得到了广泛的应用。简而言之,人脸识别技术是用摄像机或摄像头采集含有人脸的图像或视频流,并自动在图像中检测并跟踪人脸,进而对检测到的人脸的相关特征信息进行提取,然后根据相关特征信息进行识别,以此实现身份鉴别的一种新兴技术。

[0003] 目前,人脸识别技术已广泛应用于门禁设备当中,然而,在一些特殊的场合如银行、信息保密中心等,极有可能会出出现歹徒胁迫工作人员要求打开门的情况,如果该工作人员拒绝开门或者强行报警会被歹徒进行人身伤害,由此可见,现有技术中的门禁设备安全性还有待提高。

[0004] 因此,提供一种具备反胁迫功能的人脸识别门禁系统,其能够在工作人员被胁迫开门时,隐蔽通知后台管理中心,以便管理中心及时采取措施,保障工作人员的人身安全以及国家的财产安全,已经成为本领域技术人员亟待解决的技术问题。

实用新型内容

[0005] 为解决上述技术问题,本申请提供一种具备反胁迫功能的人脸识别门禁系统,其能够在工作人员被胁迫开门时,隐蔽通知后台管理中心,以便管理中心及时采取措施,保障工作人员的人身安全以及国家的财产安全,与现有技术相比,安全性得到了显著的提高。

[0006] 本申请提供的技术方案如下:

[0007] 一种具备反胁迫功能的人脸识别门禁系统,包括:中央门禁处理器;密令识别模块,用于识别接收的密令为常态正确密令或反胁迫密令,若为反胁迫密令则发送异常胁迫信号至中央门禁处理器;

[0008] 人脸识别模块,用于验证人脸信息特征通过后发送解锁指令至中央门禁处理器;

[0009] 中央门禁处理器用于接收人脸识别模块发送的解锁指令,控制门禁系统解锁;以及,用于接收密令识别模块发送的反胁迫指令,将反胁迫信息发送至后台安保中心。

[0010] 进一步地,在本实用新型一种优选的方式中,人脸识别模块包括:摄像单元,用于采集人脸图像;识别单元,用于从摄像单元采集的图像中检测识别出人脸图像;提取单元,用于从采集的图像中提取人脸图像;预处理单元,用于对提取出来的人脸图像进行预处理;计算模块,用于计算待识别人员与已录入人员特征的卡方值;匹配识别单元,用于验证待识别人员的身份,验证用户信息通过后发送发送解锁指令至中央门禁处理器。

[0011] 进一步地,在本实用新型一种优选的方式中,人脸识别模块还包括:归一化处理单元,用于对预处理后的人脸图像进行归一化处理;特征提取单元,用于从归一化的人脸图像

中提取待识别人员的特征。

[0012] 进一步地,在本实用新型一种优选的方式中,中央门禁处理器用于接收密令识别模块发送的反胁迫指令,将反胁迫信息发送至安保后台管理中心具体为:中央门禁处理器将由摄像单元采集的现场实时照片以及视频传送至后台安保中心。

[0013] 进一步地,在本实用新型一种优选的方式中,人脸识别模块还包括位姿调整提示单元,用于在人脸识别模块验证人脸特征信息失败后,发送提示验证人员调整位姿,再次进行人脸采集的提示信息。

[0014] 进一步地,在本实用新型一种优选的方式中,指纹密令识别模块包括:指纹录入单元,用于录入用户常态开锁指纹信息以及异常胁迫指纹信息;指纹识别及信息处理单元,用于识别实时输入的指纹信息为常态开锁指纹信息或异常胁迫指纹信息,若识别为异常胁迫指纹信息则向中央门禁处理器发送异常胁迫信号。

[0015] 进一步地,在本实用新型一种优选的方式中,密令识别模块具体为数字密码识别模块。

[0016] 进一步地,在本实用新型一种优选的方式中,数字信息输入部,用于输入数字信息,数字密码识别及信息处理模块,用于识别实时输入的数字信息为常态开锁密码信息或异常胁迫密码信息,若识别为异常胁迫密码信息则向中央门禁处理器发送异常胁迫信号。

[0017] 进一步地,在本实用新型一种优选的方式中,具备反胁迫功能的人脸识别门禁系统还包括验证记录保存模块,验证记录保存模块用于保存验证人员的现场验证人脸照片,以及验证时间信息。

[0018] 本实用新型提供的一种具备反胁迫功能的人脸识别门禁系统,与现有技术相比,包括:中央门禁处理器、密令识别模块与人脸识别模块,其中,密令识别模块用于识别接收的密令为常态正确密令或反胁迫密令,若为反胁迫密令则发送异常胁迫信号至中央门禁处理器;人脸识别模块,用于验证人脸信息特征通过后发送解锁指令至中央门禁处理器;中央门禁处理器用于接收人脸识别模块发送的解锁指令,控制门禁系统解锁;以及,用于接收密令识别模块发送的反胁迫指令,将反胁迫信息发送至后台安保中心。如此,若有工作人员被歹徒胁迫要求打开门时,工作人员可向密令识别模块输入反胁迫密令,密令识别模块识别为反胁迫密令则发送异常胁迫信号至中央门禁处理器,中央门禁处理器将反胁迫信息秘密发送至后台安保中心,实现反胁迫信息在不法之徒无法察觉的情况下隐蔽通知后台管理中心,有利于管理中心及时采取措施,避免了若工作人员拒绝开门或者强行报警会被歹徒进行人身伤害的危险,保障工作人员人身安全,保护国家财产安全,相较于现有技术的门禁系统而言,安全性得到了显著的提高。

附图说明

[0019] 为了更清楚地说明本申请实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本申请的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0020] 图1为本实用新型实施例提供的具备反胁迫功能的人脸识别门禁系统的示意图;

[0021] 图2为本实用新型实施例提供的具备反胁迫功能的人脸识别门禁系统的使用流程

图。

具体实施方式

[0022] 为了使本领域的技术人员更好地理解本申请中的技术方案,下面将对本申请实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本申请的一部分实施例,而不是全部的实施例。基于本申请中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本申请保护的范围。

[0023] 请如图1至图2所示,具备反胁迫功能的人脸识别门禁系统包括:中央门禁处理器1;密令识别模块2,用于识别接收的密令为常态正确密令或反胁迫密令,若为反胁迫密令则发送异常胁迫信号至中央门禁处理器1;

[0024] 人脸识别模块3,用于验证人脸信息特征通过后发送解锁指令至中央门禁处理器1;

[0025] 中央门禁处理器1用于接收人脸识别模块3发送的解锁指令,控制门禁系统解锁;以及,用于接收密令识别模块2发送的反胁迫指令,将反胁迫信息发送至后台安保中心4。

[0026] 本实用新型实施例提供的具备反胁迫功能的人脸识别门禁系统,与现有技术相比,包括:中央门禁处理器1、密令识别模块2与人脸识别模块3,其中,密令识别模块2用于识别接收的密令为常态正确密令或反胁迫密令,若为反胁迫密令则发送异常胁迫信号至中央门禁处理器1;人脸识别模块3,用于验证人脸信息特征通过后发送解锁指令至中央门禁处理器1;中央门禁处理器1用于接收人脸识别模块3发送的解锁指令,控制门禁系统解锁;以及,用于接收密令识别模块2发送的反胁迫指令,将反胁迫信息发送至后台安保中心4。如此,若有工作人员被歹徒胁迫要求打开门时,工作人员可向密令识别模块2输入反胁迫密令,密令识别模块2识别为反胁迫密令则发送异常胁迫信号至中央门禁处理器1,中央门禁处理器1将反胁迫信息秘密发送至后台安保中心4,实现反胁迫信息在不法之徒无法察觉的情况下隐蔽通知后台管理中心,有利于管理中心及时采取措施,避免了若工作人员拒绝开门或者强行报警会被歹徒进行人身伤害的危险,保障工作人员人身安全,保护国家财产安全,相较于现有技术的门禁系统而言,安全性得到了显著的提高。

[0027] 具体地,在本实用新型实施例中,人脸识别模块3包括:摄像单元,用于采集人脸图像;识别单元,用于从摄像单元采集的图像中检测识别出人脸图像;提取单元,用于从采集的图像中提取人脸图像;预处理单元,用于对提取出来的人脸图像进行预处理;计算模块,用于计算待识别人员与已录入人员特征的卡方值;匹配识别单元,用于验证待识别人员的身份,验证用户信息通过后发送发送解锁指令至中央门禁处理器1。

[0028] 具体地,在本实用新型实施例中,人脸识别模块3还包括:归一化处理单元,用于对预处理后的人脸图像进行归一化处理;特征提取单元,用于从归一化的人脸图像中提取待识别人员的特征。

[0029] 具体地,在本实用新型实施例中,中央门禁处理器1用于接收密令识别模块2发送的反胁迫指令,将反胁迫信息发送至安保后台管理中心具体为:中央门禁处理器1将由摄像单元采集的现场实时照片以及视频传送至后台安保中心4。在本实施例中,中央门禁处理器1可将现场的实时照片和视频主动传送至后台安保中心4,从而有利于供安保中心根据现场情况进行最优的处警处理方案。

[0030] 具体地,在本实用新型实施例中,人脸识别模块3还包括位姿调整提示单元,用于在人脸识别模块3验证人脸特征信息失败后,发送提示验证人员调整位姿,再次进行人脸采集的提示信息。

[0031] 具体地,在本实用新型实施例中,指纹密令识别模块2包括:指纹录入单元,用于录入用户常态开锁指纹信息以及异常胁迫指纹信息;指纹识别及信息处理单元,用于识别实时输入的指纹信息为常态开锁指纹信息或异常胁迫指纹信息,若识别为异常胁迫指纹信息则向中央门禁处理器1发送异常胁迫信号。

[0032] 具体地,在本实用新型实施例中,密令识别模块2具体为数字密码识别模块。

[0033] 具体地,在本实用新型实施例中,数字信息输入部,用于输入数字信息,数字密码识别及信息处理模块,用于识别实时输入的数字信息为常态开锁密码信息或异常胁迫密码信息,若识别为异常胁迫密码信息则向中央门禁处理器1发送异常胁迫信号。

[0034] 在本实施例中,涉及两种反胁迫模式,第一种为将指纹模块嵌入人脸识别门禁设备,用户登记人脸特征信息,正常指纹信息和胁迫指纹信息并保存至门禁设备。用户若遇到被歹徒胁迫的紧急情况,先输入胁迫指纹,验证成功后触发反胁迫报警并将报警信息悄无声息地发至管理平台,然后用户与门禁设备里保存的人脸特征信息进行比对,比对成功后开门。

[0035] 第二种为用户预设反胁迫按键,正常情况按正常开门模式的按键,胁迫模式按预设的胁迫键,系统自动判定,出现胁迫情况时隐蔽后台告警。

[0036] 其中,更为具体地,第一种方式为将指纹模块嵌入至人脸识别门禁设备,人脸识别门禁录入用户的人脸特征信息同时,再录入用户的正常指纹信息和胁迫指纹信息。用户开门使用正常指纹+人脸识别方式,若遇到被歹徒胁迫的紧急情况,先输入胁迫指纹,验证成功后启动人脸认证,认证通过后后台隐蔽告警,并将现场的实时照片和视频主动传送至后台安保中心4,供安保中心根据现场情况进行最优的处警处理方案。

[0037] 第二种方式为人脸识别设备具备4*4的数字键盘,系统具备胁迫告警的设置菜单,用户可以自定义正常开门的键值以及胁迫开门的键值。当正常开门键值触发后,进行人脸认证,认证通过后仅开锁。当胁迫开门键值触发后,进行人脸认证,后台隐蔽告警,并将现场的实时照片和视频主动传送至后台安保中心4,供安保中心根据现场情况进行最优的处警处理方案。

[0038] 当设定人脸识别处于胁迫状态时,设备关闭了人脸检测开始认证的方式,必须接收到按键或者接收到指纹才可启动,避免了胁迫情况发生时无法启动告警。

[0039] 具体地,在本实用新型实施例中,具备反胁迫功能的人脸识别门禁系统还包括验证记录保存模块,验证记录保存模块用于保存验证人员的现场验证人脸照片,以及验证时间信息。

[0040] 此外,本申请实施例还涉及具备反胁迫功能的人脸识别门禁系统的使用流程方法,具体包括以下步骤:

[0041] 步骤一:用户登记,管理员人脸认证进入用户管理菜单,给当前用户登记人脸特征,人脸特征登记完成后,选择此用户,进行胁迫指纹和正常开门指纹的登记,此方式不同用户对应不同的胁迫指纹。

[0042] 步骤二:胁迫键值设定,管理员人脸认证进入到设置菜单,配置好正常开门键值以

及胁迫开门键值,此方式所有开门用户均采用同样的键值正常开门或者胁迫开门。

[0043] 步骤三:胁迫模式开启,管理员人脸认证进入设置菜单,将此设备启动模式设置为反胁迫,反胁迫模式开启后,设备关闭了人脸检测自启动功能,进入到接收到正常开门指令或者胁迫开门指令方会启动人脸认证模式。

[0044] 步骤四:正常开门流程,用户输入正常开门按键或者输入正常开门指纹,人脸认证通过,开启门锁,记录现场开门照片和时间地点。

[0045] 步骤五:胁迫情况开门流程,用户输入胁迫开门按键或者输入胁迫开门指纹,人脸验证成功后触发后台隐秘的反胁迫告警,并将人脸设备所拍摄的现场照片和视频发送至安保中心,安保中心看到现场情况后,进行合理的胁迫处理方案,告警同时设备控制门锁开启,以保障现场工作人员安全与国家财产安全。

[0046] 对所公开的实施例的上述说明,使本领域专业技术人员能够实现或使用本实用新型。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的,本文中所定义的一般原理可以在不脱离本实用新型的精神或范围的情况下,在其它实施例中实现。因此,本实用新型将不会被限制于本文所示的这些实施例,而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

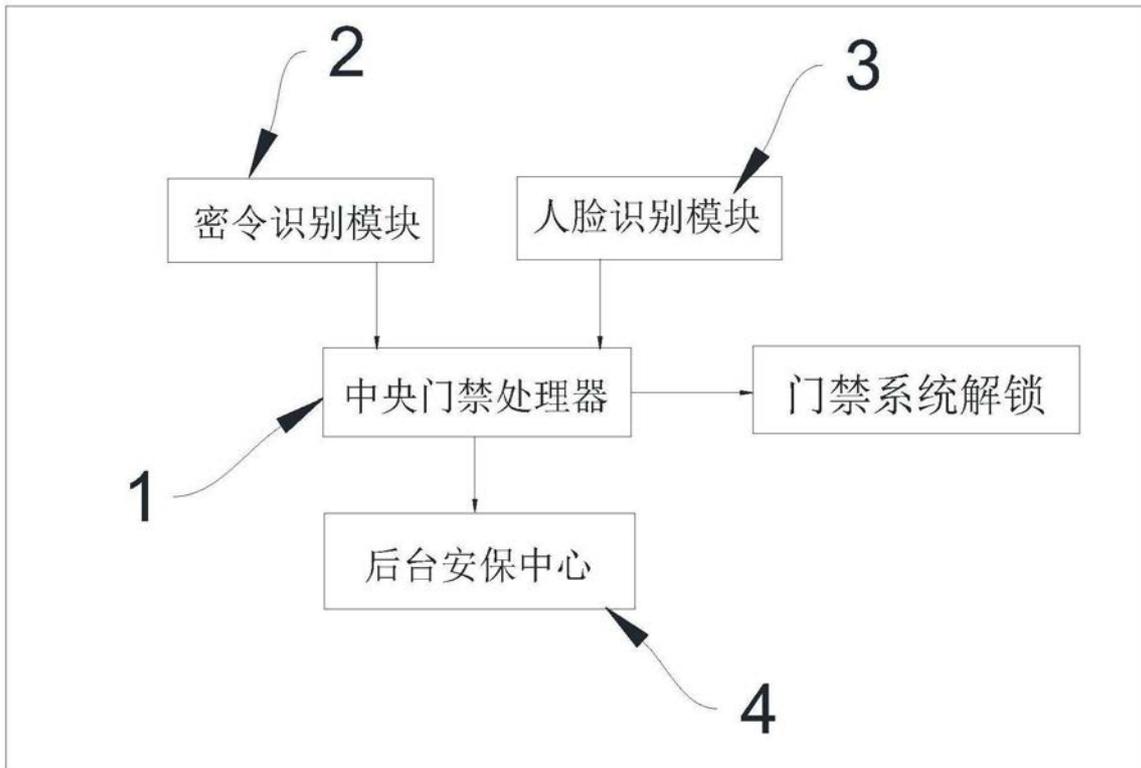


图1

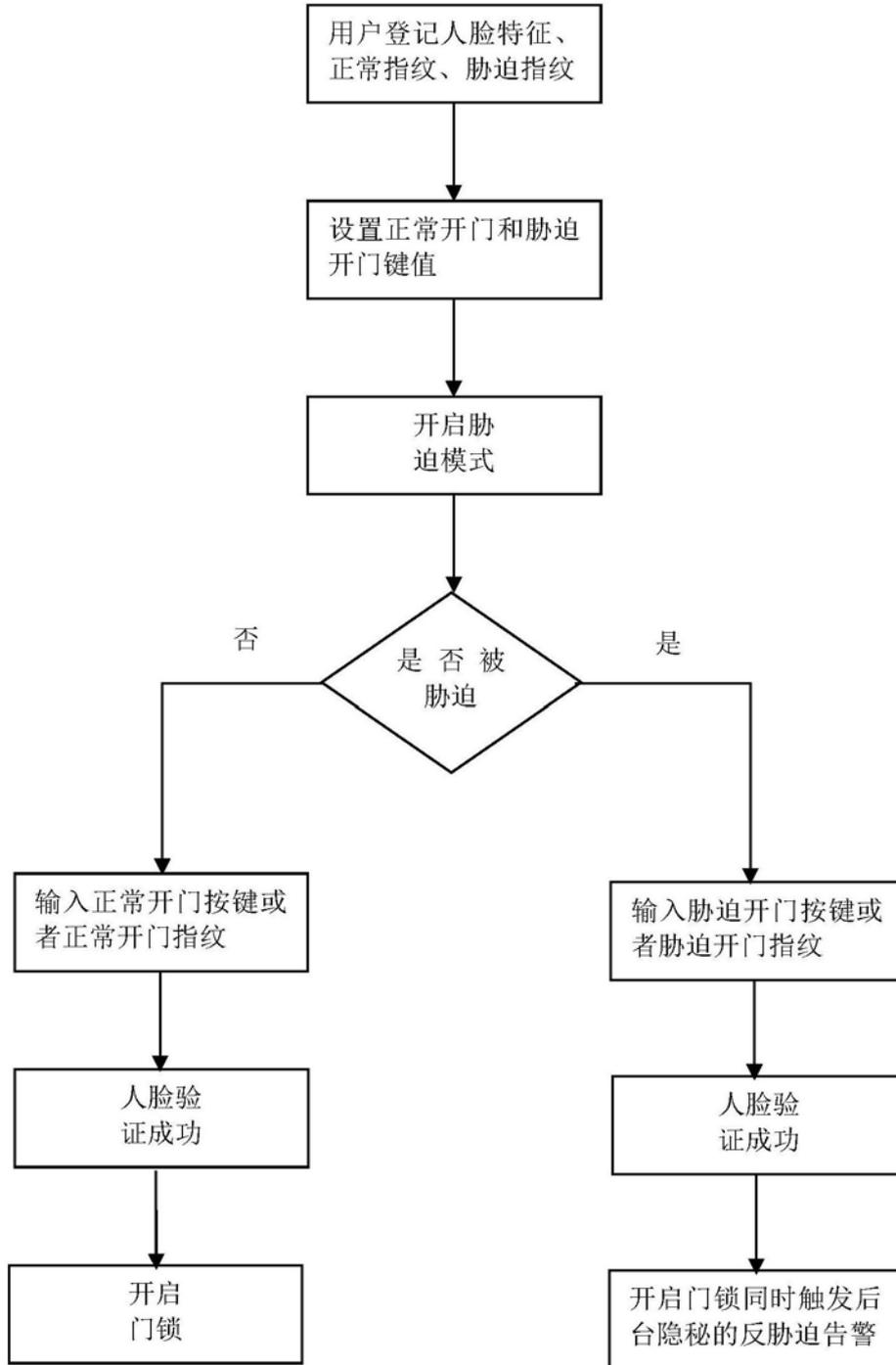


图2